4.(AMENDED) The method as claimed in claim 1, [characterized in that] wherein a prohibition of playing [(24)] of said digital data is delivered when:

- an encryption [(2)] of said digital data has not been identified; and
- a watermarking [(3)] of said digital data has been identified.

5.(AMENDED) The method as claimed in claim 1, [characterized in that] wherein a prohibition of copying [(27)] is delivered [(26)] when:

- an encryption [(2)] of said digital data has been identified;
- a watermarking [(3)] of said digital data has been identified; and
- a recordable type of carrier [(11)] has been identified.

6.(AMENDED) The method as claimed in claim 1, [characterized in that] wherein a prohibition of copying [(27)] is delivered [(28)] when:

- an encryption [(2)] of said digital data has been identified;
- a watermarking [(3)] of said digital data has been identified;
- a non-recordable type of carrier [(11)] has been identified; and
- no cryptographic signature [(16)] accompanying said digital data has been identified.

7.(AMENDED) The method as claimed in [one of claims 1, 2, 5 or 6, characterized in that] claim 1, wherein it comprises:

- a conversion [(30)] of the digital data [(29)] into analog signals [(31)]; and
- a corruption [(33)] of the analog signals if a prohibition of digital copying [(27)] is delivered.

8.(AMENDED) The method of protection according to [either of claims 5 or 6, characterized in that] claim 5, wherein the prohibition of digital copying [(27)] comprises a blocking [(35)] of output of the digital data.

9.(AMENDED) A device for playing digital data stored on an information carrier comprising at least:

- a digital output [(43)] for delivering signals representative of the digital data upon playing said digital data;

an analog output [(44)] for delivering analog signals representative of the digital data upon playing said digital data;

means [(45)] for detecting:

- an encryption of said digital data;
- a watermarking of said digital data;
- a recordable or non-recordable type of said information carrier;
- a cryptographic signature accompanying said digital data;
- a system for decrypting said digital data when an encryption is detected;

a system for protection [(46)] against the copying of said digital data receiving signals from said detection means [(45)] and generating a copy permission signal [(22)] or a copy prohibition signal [(27)] by employing the method according to [one of claims 2 and 4 to 6] claim 2;

recording control means [(47)] blocking the signals delivered at the digital output [(43)] when said control means receive a copy prohibition signal [(27)] from the protection system [(46)];

a system for protection [(46)] of playing receiving signals from said detection means [(45)] and generating a playing prohibition signal [(24)] by employing the method according to claim 3; and

playing control means [(48)] interrupting the playing of the data or their output to the analog output [(44)] when said monitoring means receive a playing prohibition signal from the protection system [(46)].

A3 cncld.